

Claims

1. A method to delivery encrypted digital content from a first system for playing the content to a second system for playing the content, the method on a second system comprising the steps of:
reading on a second system from a computer readable medium metadata which has previously been associated, wherein in the content is encrypted with a first key associated with the first system;

selecting from the metadata associated content to decrypt;
establishing a secure transmission with an authorization authority for decrypting the content;
and

receiving a decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted.

2. The method according to claim 1, further comprising the steps of:
playing at least part of the previously encrypted content by decrypting the encrypted content with the decrypting key.

3. The method according to claim 2, wherein the step of decrypting is performed in a tamper-resistant environment for deterring unauthorized access to the decrypting key.

4. The method according to claim 1, wherein the step of decrypting further comprises:
decrypting at least part of the previously encrypted content as permitted;
reencrypting the decrypted content utilizes a unique local decrypting key;
storing the content in a library; and
decrypting at least part of the content from the library using the unique local decrypting key

$\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{x}} \right) = \frac{\partial L}{\partial x}$

EXPRESS MAIL LABEL NO. EL563155121US

1 6. A method to delivery encrypted digital content from a first end user system for playing the
2 content to a second end user system for playing the content, the method on the first end user system
3 comprising the steps of:

4 reading from a computer readable medium metadata which has previously been associated
5 with the content;

6 selecting from the metadata associated content to decrypt;

7 establishing a secure connection with an authorization authority for decrypting the content;

8 receiving a secure container containing the decrypting key for decrypting at least part of the
9 previously encrypted content as permitted;

10 creating an secure container using the encrypting key from a clearinghouse, wherein the
11 secure container has an encrypting key therein from the first end user system;

12 transferring the secure container to the clearinghouse for authentication of permission to
13 decrypt the content;

14 receiving from the clearinghouse, a secure container encrypted using the encrypting key of
15 the first end user system containing the decrypting key for decrypting at least part of the previously
16 encrypted content stored on the computer readable medium as permitted; and

17 creating a container for distribution to a second end user system for playing the content which
18 has been reencrypted with a new encrypting key associated with the first end user system.

1 7. The method according to claim 6, wherein the step of playing further comprises playing at
2 least part of the previously encrypted content comprising a plurality of distinct titles whereby each
3 distinct title is decrypted with a unique decrypting key.

1 8. The method according to claim 6, wherein the step of establishing a secure connecting further
2 comprises the step of transmitting a credit information to the authorization authority.

EXPRESS MAIL LABEL NO. EL563155121US

- 1 9. The method according to claim 6, wherein the metadata is stored as part of a promotional
2 package on a CD or DVD containing non-encrypted content.

Chemical shift, δ , ppm	Assignment	Chemical shift, δ , ppm	Assignment
12.0-12.5	Carbonyl	12.0-12.5	Carbonyl
10.0-10.5	Aldehyde	10.0-10.5	Aldehyde
8.0-8.5	Aromatic	8.0-8.5	Aromatic
7.0-7.5	Vinyl	7.0-7.5	Vinyl
6.0-6.5	Alkene	6.0-6.5	Alkene
5.0-5.5	Alkyne	5.0-5.5	Alkyne
4.0-4.5	Alcohol	4.0-4.5	Alcohol
3.0-3.5	Ether	3.0-3.5	Ether
2.0-2.5	Alkane	2.0-2.5	Alkane
1.0-1.5	Methyl	1.0-1.5	Methyl

EXPRESS MAIL LABEL NO. EL563155121US

1 10. A computer readable medium containing programming instructions for delivery of encrypted
2 digital content from a first system for playing the content to a second system for playing the content,
3 the programming instructions for execution on a second user system comprising:

4 reading on a second system from a computer readable medium metadata which has
5 previously been associated, wherein in the content is encrypted with a first key associated with the
6 first system;

7 selecting from the metadata associated content to decrypt;

8 establishing a secure transmission with an authorization authority for decrypting the content;

9 receiving a decrypting key for decrypting at least part of the previously encrypted content
10 stored on the computer readable medium as permitted.

1 11. The computer readable medium according to claim 10, wherein the programming instruction
2 of decrypting is performed in a tamper-resistant environment for deterring unauthorized access to
3 the decrypting key.

1 12. The computer readable medium according to claim 10, wherein the programming instruction
2 of decrypting further comprises:

3 decrypting at least part of the previously encrypted content as permitted;

4 reencrypting the decrypted content utilizes a unique local decrypting key;

5 storing the content in a library; and

6 decrypting at least part of the content from the library using the unique local decrypting key.

1 13. The computer readable medium according to claim 12, wherein the programming instruction
2 of decrypting and reencrypting is performed in a tamper-resistance environment for deterring
3 unauthorized access to the decrypting key.

EXPRESS MAIL LABEL NO. EL563155121US

1 14. A computer readable medium containing programming instructions for delivering encrypted
2 digital content from a first end user system for playing the content to a second end user system for
3 playing the content, the programming instructions for execution on a first user system comprising:
4 reading from a computer readable medium metadata which has previously been associated
5 with the content;
6 selecting from the metadata associated content to decrypt;
7 establishing a secure connection with an authorization authority for decrypting the content;
8 receiving a secure container containing the decrypting key for decrypting at least part of the
9 previously encrypted content as permitted;
10 creating an secure container using the encrypting key from a clearinghouse, wherein the
11 secure container has an encrypting key therein from the first end user system;
12 transferring the secure container to the clearinghouse for authentication of permission to
13 decrypt the content;
14 receiving from the clearinghouse, a secure container encrypted using the encrypting key of
15 the first end user system containing the decrypting key for decrypting at least part of the previously
16 encrypted content stored on the computer readable medium as permitted; and
17 creating a container for distribution to a second end user system for playing the content which
18 has been reencrypted with a new encrypting key associated with the first end user system.

1 15. The computer readable medium according to claim 14, wherein the programming instruction
2 of playing further comprises playing at least part of the previously encrypted content comprising a
3 plurality of distinct titles whereby each distinct title is decrypted with a unique decrypting key.

1 16. The computer readable medium according to claim 14, wherein the programming instruction
2 of establishing a secure connecting further comprises the step of transmitting a credit information
3 to the authorization authority.

- [illegible]

EXPRESS MAIL LABEL NO. EL563155121US

1 18. A first end user system for delivery of encrypted digital content to a second end user system
2 for playing the content, the first end user system comprising:
3 an interface for reading from a computer readable medium metadata which has previously
4 been associated with the content;
5 an input device for receiving at least one selection from the metadata associated content to
6 decrypt;
7 a network connection for establishing a secure connection with an authorization authority for
8 decrypting the content;
9 a first secure container received from the computer readable medium containing the
10 decrypting key for decrypting at least part of the previously encrypted content as permitted;
11 a tamper resistant environment for creating a second secure container using the encrypting
12 key from a clearinghouse, wherein the second secure container has an encrypting key therein from
13 the first end user system; wherein the second secure container is subsequently transferred over the
14 network connection to the the clearinghouse for authentication of permission to decrypt the content;
15 a third secured container received from the clearinghouse, wherein the third secured container
16 is encrypted using the encrypting key of the first end user system containing the decrypting key for
17 decrypting at least part of the previously encrypted content stored on the computer readable medium
18 as permitted; and
19 a fourth secured container created in the tamper resistant environment for distribution to a
20 second end user system for playing the content which has been reencrypted with a new encrypting
21 key associated with the first end user system.